

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2002年10月15日

出 願 番 号

Application Number:

特願2002-300108

[ST.10/C]:

[JP2002-300108]

出 願 人

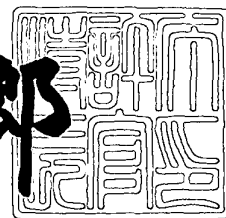
Applicant(s):

松下電器産業株式会社

2003年 7月 1日

特 許 庁 長 官
Commissioner,
Japan Patent Office

太田信一郎



出証番号 出証特2003-3051955

【書類名】 特許願

【整理番号】 2032740087

【提出日】 平成14年10月15日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 9/00

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 杉山 圭司

【発明者】

【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内

【氏名】 ▲たか▼尾 直弥

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100097445

【弁理士】

【氏名又は名称】 岩橋 文雄

【選任した代理人】

【識別番号】 100103355

【弁理士】

【氏名又は名称】 坂口 智康

【選任した代理人】

【識別番号】 100109667

【弁理士】

【氏名又は名称】 内藤 浩樹

【手数料の表示】

【予納台帳番号】 011305

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9809938

【書類名】 明細書

【発明の名称】 グループ検索方法、グループ情報入手方法およびエントリポイント検索方法

【特許請求の範囲】

【請求項 1】 検索者が P 2 P ネットワーク上に存在するグループに参加するための情報を入手するための検索手段であって、
ネットワーク上に存在するグループを特定するための情報を含むグループ情報入手するグループ情報入手ステップと、
入手したグループ情報に対応するグループのエントリポイントの情報を入手するエントリポイント入手ステップと、
を実行することを特徴とするグループ検索方法。

【請求項 2】 検索者がグループを検索するためのグループ検索メッセージを生成し、
問い合わせを行うグループ情報検索ステップと、
グループ検索メッセージを受け取った応答者が、グループ公開鍵を含むグループ情報を検索者に送信するためのグループ情報応答メッセージを生成し、応答を行うグループ情報応答ステップと、
を実行することを特徴とするグループ情報入手方法。

【請求項 3】 前記グループ情報応答ステップにおいて、
グループ管理者が保持するグループ秘密鍵に基づいてグループ情報応答メッセージを生成することを特徴とする第 2 の請求項記載のグループ情報入手方法。

【請求項 4】 前記グループ情報応答ステップにおいて、グループ管理者からグループ参加証発行許可証の発行をうけた発行者が、
グループ参加証発行許可証に含まれる公開鍵に対応する秘密鍵に基づいてグループ情報応答メッセージを生成することを特徴とする第 2 の請求項記載のグループ情報入手方法。

【請求項 5】 検索者がグループ公開鍵を含むグループ情報に基づいてエントリポイント検索メッセージを生成し、
問い合わせを行うエントリポイント検索ステップと、

前記エントリポイント検索メッセージを受信した応答者が受信したエントリポイント検索メッセージに対応するグループのエントリポイントの情報を含むエントリポイント検索応答メッセージを生成し、

応答を行うエントリポイント検索応答ステップと、
 を行うことを特徴とするエントリポイント検索方法。

【請求項 6】 前記エントリポイント検索応答ステップにおいて、エントリポイント検索メッセージの受信者が、エントリポイント検索メッセージに含まれるグループ公開鍵と応答者が保有するグループ公開鍵の比較によって、検索者の要求しているグループと応答者が所属しているグループの一意性を確認することを特徴とする請求項 5 記載のエントリポイント検索方法。

【請求項 7】 前記エントリポイント検索応答ステップにおいて、エントリポイント検索メッセージの受信者が、エントリポイント検索メッセージに含まれるグループ公開鍵と応答者が保有するグループ公開鍵の比較だけでなく、検索メッセージに含まれるグループ公開鍵が、応答者が保有するグループ公開鍵更新履歴との比較によって、検索者の要求しているグループと応答者が所属しているグループの一意性を確認することを特徴とする請求項 5 記載のエントリポイント検索方法。

【請求項 8】 前記エントリポイント検索応答ステップにおいて、グループの一意性が確認でき、かつエントリポイント検索メッセージに含まれるグループ公開鍵が、応答者の保有する最新のグループ公開鍵でない場合に、最新のグループ公開鍵を通知することを特徴とする請求項 7 記載のエントリポイント検索方法。

【請求項 9】 前記エントリポイント検索応答ステップにおいて、応答者がグループ参加証、および応答者の秘密鍵に基づいてエントリポイント検索応答メッセージを生成することを特徴とする請求項 5 記載のエントリポイント検索方法。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、ネットワークで接続された機器によって構成されるグループに関する情報を取得するための検索方法に関する。

【0002】

【従来の技術】

インターネットに接続してネットワークサービスを楽しむユーザ数は、接続機器や接続料金の廉価化、接続機器の多彩化、および通信速度の向上などにより急速に増加している。インターネット普及当初は、一部の情報提供者が提供する情報を一般ユーザがダウンロードする一方向のサービスが主流であったが、現在は自分の持つ情報、すなわちテキストデータ、静止画像データ、音声データ、動画データなどを発信したいという。

【0003】

一般ユーザも増え、主にWWW (World Wide Web) などのサーバに自分の情報を複製し、他のユーザが閲覧可能とすることによってこれを実現している。

【0004】

サーバで情報を公開するにあたっては、大きく分けて(1)サーバを自分で運用する、(2)サービス提供者が有料または無料で提供しているサーバに情報をアップロードする、という二つの方法がある。さらに、不特定多数を対象に発信するのではなく、友人・家族・共通の趣味を持つ者など特定ユーザ間(以下グループと呼ぶ)でのみプライベートな情報を共有したいという要求も増えているが、これを実現する方法としては、主に認証サーバを用いる方法、すなわちグループへの参加を認められたユーザのユーザIDとパスワードの組(以下グループリスト)を認証サーバ(情報提供サーバと同一であっても良い)に登録しておき、ユーザが入力したユーザIDとパスワードの組を確認することによって当該グループでの情報共有を許可する方法などが用いられている。

【0005】

また、作成したグループを公開する際にも、グループに関する情報、つまりグループのカテゴリやメンバの情報、参加のための条件などを登録サーバに登録することにより、不特定多数のユーザに参加を呼びかけることが多い。ユーザは登録サーバにアクセスすることによって、登録されているグループの存在を知り、グループへの参加に必要な情報を入手する。チャット、BBS、メーリングリス

トなどのネットワーク上でのコミュニケーションを行うことを目的とするグループの多くはこのような方法で、グループを公開する。

【0006】

このように情報提供者はサーバに情報を格納しておき、情報受信者がサーバへアクセスするというモデル（サーバクライアントモデルと呼ぶ）には、次の問題点がある。

【0007】

すなわち、自分でサーバを運用する場合には、

（１）高度な知識が必要：サーバやネットワーク等に関する十分な知識が必要とされ、一般ユーザが運用することは困難な場合が多い、

（２）コストがかかる：機材やソフトウェア以外にも、基本的に常時サービスを提供するためにサーバを常時稼働させるための運用費が必要となる、

などの問題点があり、有料または無料で提供されるサーバを利用する場合には、

（３）容量制限：多くの場合サーバに格納できる情報の容量には制限が設けられており、有料サーバの場合はコストをより多く負担することで容量制限を緩和することができるが、その場合にはより多くのコストがかかる、

（４）プライバシー：サーバ提供者が信頼に足る場合であっても、何らかの事故等でサーバに格納した情報が第三者に漏れる場合があり、真にプライバシー保護を必要とする情報を共有することは困難である、

などの問題点があり、共通の課題としては、

（５）信頼性：サーバが何らかのトラブルでアクセス不能になった場合、情報発信や情報共有はまったく不可能となる、

という問題点がある。

【0008】

なお、上で述べたコストに関する問題については、情報提供に対する収入によりコストを回収できるならば一定の負担は問題とならないが、一般ユーザが個人情報を発信あるいは共有する多くの場合はこれに当てはまらない。

【0009】

上記のようなサーバクライアントモデルにおける情報共有時の問題点を解消

するために近年着目されているのがピアートゥーピア（Peer-to-Peer、以下P2P）モデルである。これは、情報をサーバに一極集中させず、必要ときに情報発信者－情報受信者間で直接伝送することで上記問題点を解決するものである（例えば、非特許文献1参照）。

【0010】

P2Pモデルのネットワーク（以下P2Pネットワーク）に参加しているユーザ間で情報を転送する場合の流れを図10にて例示する。

【0011】

各ユーザはP2Pネットワークに参加している他のユーザの存在を一人以上知っており、例えばAはBとF、BはAとCとD、EはDのみの存在を知っている。この状態でAが欲する情報を受信する際には、まず情報を持つユーザを特定するために検索を行う。Aはまず自分の知っているBとFに検索要求を発する。次にBとFはそれぞれが知っているユーザにこの検索要求を中継し、その先のユーザも同様に中継する（ステップ1001）。そして、この検索要求に合致する情報を持っているユーザ、この場合はCとEは、Aに対して情報を持っていることを直接通知し（ステップ1002）、Aは何らかの判断基準でEを選択してAとEの間で情報の転送が直接行われる（ステップ1003）。もちろん情報を分割してCとEの両者から同時に転送することも可能である。これにより、前記サーバクライアントモデルの問題点（1）～（5）は次のように解決される。

【0012】

（1）サーバを運用しないため高度な知識は必要とされない。

【0013】

（2）またサーバを運用または利用するためのコストも不要である。

【0014】

（3）情報発信者Eから直接情報Aを受信するので、転送可能な情報の容量はAとEのローカルな記録容量のみに制約され、実質的に容量の制限はない。

【0015】

（4）転送される情報はAとE以外の第三者を経由しないので、既存技術でAとEの間の通信路を暗号化するなどすれば情報のプライバシーは保たれる。

【0016】

(5) 仮にEがネットワークに参加していない状態（オフライン）であっても、AはCから必要な情報を得ることができる。

【0017】

さて、P2Pネットワークにおいてグループでの情報共有を行う場合には登録サーバといった、グループに関する情報を管理しているサーバが存在しないので、グループに参加するユーザは、何らかの別の方法でグループに関する情報を入手する必要がある。

【0018】

その際には、上記で述べたP2Pモデルによる情報伝達の手法を用いることができる。グループに関する情報を入手するための検索をP2Pネットワークによって実行することにより、登録サーバを使用することなく、ネットワーク上に存在するグループの情報を入手することが出来る。

【0019】

ユーザは、まず

- (1) ネットワーク上に存在するグループを識別するための情報および
- (2) グループを分類するための属性などに関する情報を入手し、次に
- (3) グループの参加するための場所に関する情報

を入手する必要がある。

【0020】

(1) の情報はグループに与えられたIDなどであり、グループを一意に指定できる情報である。

【0021】

(2) の情報はグループのカテゴリ、活動目的、グループへの参加条件などである。

【0022】

(3) グループのメンバのIPアドレス、ポート番号などであり、実際にグループのメンバにアクセスするために必要な情報である。

【0023】

本発明では以後（１）の情報をグループ識別情報、（２）の情報をグループ属性情報、（３）の情報をエントリポイント情報と呼ぶ。また、（１）および（２）の情報をまとめたものをグループ情報と呼ぶ。

【0024】

ユーザはまず、検索によってグループ識別情報および、グループ属性情報を入手し、入手したグループ属性情報から、そのグループに参加するかどうかを判断する。そのグループに参加する場合には、グループのエントリポイント情報を検索によって入手する。この際に、先に入手しているグループ識別情報によって、どのグループのエントリポイントが必要であるのかを指定する。エントリポイント情報を入手したユーザは、該当するエントリポイントにアクセスすることによってグループの活動に参加する。上記の処理をP2Pネットワークの検索手段を用いて行う場合、登録サーバなどによってグループ情報が管理されていないことにより、二つの問題が生じうる。

【0025】

第一の問題は、グループ情報の詐称である。図11において、ネットワーク上に3つのグループG1、G2、G3が存在している。ここで、ユーザAは自分がもとめるグループの条件 α を作成し、P2Pネットワークに対してグループ情報の検索を行う（ステップ1101）。

【0026】

次にB、FはAからの検索をうけとり、自分の属するグループのグループ情報から、自分の属するグループがAの指定した条件 α 適合するかを判定する。この例では、G2は条件 α に適合しないため、B、Fはそれぞれ自分が知っているユーザに検索を転送する。そして、条件 α に適合するグループのメンバ、この場合はC、Dは自分が保有するグループのグループ識別情報DI1および、グループ属性情報AI1を、Aに通知する（ステップ1102）。この場合にはAは自分の指定する条件に合うグループの存在を知り、参加することができる。

【0027】

しかし、P2Pネットワークでは、図12に示すように容易にグループ情報の詐称を行うことができる。ユーザAは自分がもとめるグループの条件 α を作成し

、P2Pネットワークに対して検索を行う（ステップ1201）。

【0028】

この検索に対する応答として下記のような不正な応答が返される可能性がある。

【0029】

(1) 自分のグループに関するグループ属性情報を詐称する。

【0030】

Bは、応答として自己のグループ識別情報DI2を使用し、それに対応するグループ属性情報として、自己のグループのグループ属性情報DI2ではなく、条件 α に適合する。別のグループのグループ属性情報AI1を、使用してAに送信する（ステップ1202）。この場合、Aは自分の条件に合わないグループG2に参加してしまう可能性がある。

【0031】

(2) 他のグループのグループ識別情報を使用し、そのグループに関するグループ属性情報を詐称する。Eは、他のグループのグループのグループ識別情報DI1を使用し、条件 α に適合するようグループ属性情報AI4を捏造して、Aに送信する。（ステップ1203）AはグループG1に関して誤ったグループ属性情報を入手してしまい、かつ、グループG1は自己のグループについて誤ったグループ属性情報AI4を広められる危険性がある。また、エントリポイント情報を検索する際にも、同様に情報の詐称を行うことができる。

【0032】

エントリポイント情報をP2Pネットワークの検索手段を使用して、検索する場合の処理の流れは図11とほぼ同様である。検索するユーザは条件 α として、情報を入手したいグループのグループ識別情報を指定する。指定されたグループ識別情報によって特定されるグループに属しているユーザは、その検索に対する応答として、自身のエントリポイントの情報を応答として返す。

【0033】

この際にも、グループ識別情報とエントリポイント情報の対応がサーバによって管理されていないために容易に、検索に対して不正な応答を返すことができる。

。この場合には、下記の不正な応答が想定できる。

【0034】

(3) 他のグループのグループ識別情報を使用し、そのグループに関するエントリポイント情報を詐称する。EがグループG1のエントリポイント情報の検索に対して、G1のエントリポイント情報として、Bのエントリポイント情報を返すことができる。この場合、AはグループG1とは異なるG2参加してしまう可能性があり、グループG2のメンバBはAからの誤ったアクセスを処理しなければならない可能性がある。

【0035】

上記のうち、(1)についてはサーバ・クライアントモデルについても起こりうる問題であるが、(2)(3)については、P2P環境においてより、生じやすい問題である。サーバによってグループ識別情報とグループ属性情報の対応、および、グループ識別情報とエントリポイント情報の対応が管理されていないため、悪意のあるユーザは、あるグループ識別情報によって識別されるグループのグループ属性情報やエントリポイント情報を改竄、捏造して検索として応答することが容易にできる。

【0036】

このとき、応答を受け取ったユーザは、その対応が正しいものかを判断する方法が現在のP2Pネットワークによる情報検索では与えられていない。これは、従来のP2Pネットワークにおける検索手段では、検索者の検索に対し、任意の応答者が応答を返すことができることに原因がある。

【0037】

第二の問題点は、グループに関する一意性である。グループが登録サーバによって一元的に管理されている場合、二つのグループを識別するための識別子はサーバによって容易に生成することができる。ユーザはこの識別子をグループ識別情報として使用することで、自分が情報を入手したいグループを一意に特定することができる。

【0038】

しかし、P2Pネットワークにおいて、誰もが自由にグループを生成する場合

、各グループを一意に識別するための識別子を生成することは容易ではない。ユーザAがグループを生成し、そのグループに識別子G1を与える。その後、ユーザBもグループを生成し、そのグループの識別子としてG1を与えたとする。この時、別のユーザCはG1という識別子によって、ユーザAの生成したグループと、ユーザBの生成したグループを識別することが出来ない。特に、ユーザBが故意にユーザAと同じグループの識別子を利用する事態が想定されるため、単に識別子の生成方法だけでは、この第二の課題を解決することはできない。故に、P2Pネットワークでグループを運用する際に、グループ識別情報として何を用いるべきかは大きな課題の一つである。

【0039】

上記の第一、第二の課題を解決するために、グループやユーザに関する情報はサーバを使用することによって管理し、実際のデータ転送などをP2Pで行うといったアプローチを用いることもできる。この手法はHybrid型P2Pと呼ばれ、前記サーバクライアントモデルの課題(3)および(4)を改善することができ、グループに関する情報の詐称を防ぐことができ、グループの一意性を確保することも容易にする。

【0040】

しかし、サーバを導入することによって前記サーバクライアントモデルの課題(1)、(2)、(5)の問題点を解決できなくなる。

【0041】

【非特許文献1】

小柳恵一編著、「P2P インターネットの新世紀」、オーム社、2002年5月1日

【0042】

【発明が解決しようとする課題】

以上述べたように、サーバクライアントモデルの問題点を解決するためのP2Pネットワークにおいてグループでの情報共有を行う場合、

(1) グループ情報を管理するサーバを使用しない場合、情報を容易に改竄することができるため、検索に対する応答に信頼性がなくなるといった問題点があり

、（２）グループを一意に指定する識別子の生成が容易ではないといった問題点がある。また、（３）グループ情報を管理するサーバを使用する方法では運用コスト、信頼性といった問題点がある。

【0043】

本発明は、上記問題点に鑑み、グループでの情報共有にサーバの運用を必要とせず、かつグループに関する情報を改竄することができず、かつグループの一意性を判断することができるグループ検索方法を提供することを目的とする。

【0044】

【課題を解決するための手段】

本発明は、以上述べた課題を解決するため、以下のような構成をとるグループ情報入手方法、エントリポイント情報入手方法からなるグループ検索方法を提供する。

【0045】

グループ検索方法の一実施形態は、ネットワーク上に存在するグループに参加するために必要な情報を含むグループ情報を入手するグループ情報入手ステップと、入手したグループ情報に対応するグループのエントリポイントを手入するエントリポイント情報入手ステップと、を実行することを特徴とする。

【0046】

グループ情報入手方法の一実施形態は検索者がグループを検索するためのグループ検索メッセージを生成し、問い合わせを行うグループ情報検索ステップと、グループ検索メッセージを受け取った応答者が、グループ公開鍵を含むグループ情報を検索者に送信するためのグループ情報応答メッセージを生成し、応答を行うグループ情報応答ステップと、を実行することを特徴とする。

【0047】

また、グループ情報入手方法の一実施形態は、前記グループ情報応答ステップにおいて、グループ管理者が保持するグループ秘密鍵に基づいてグループ情報応答メッセージを生成することを特徴とする。

【0048】

また、グループ情報入手方法の一実施形態は、前記グループ情報応答ステップ

において、グループ管理者からグループ参加証発行許可証の発行をうけた発行者が、グループ参加証発行許可証に含まれる公開鍵に対応する秘密鍵に基づいてグループ情報応答メッセージを生成することを特徴とする。

【0049】

エントリポイント情報入手方法の一実施形態は検索者がグループ公開鍵を含むグループ情報に基づいてエントリポイント検索メッセージを生成し、問い合わせを行うエントリポイント検索ステップと、前記エントリポイント検索メッセージを受信した応答者が受信したエントリポイント検索メッセージに対応するエントリポイント検索応答メッセージを生成し、応答を行うエントリポイント検索応答ステップと、を行うことを特徴とする。

【0050】

また、エントリポイント入手方法の一実施形態は、前記エントリポイント検索応答ステップにおいて、エントリポイント検索メッセージの受信者が、エントリポイント検索メッセージに含まれるグループ公開鍵と応答者が保有するグループ公開鍵の比較によって、検索者の要求しているグループと応答者が所属しているグループの一意性を確認することを特徴とする。

【0051】

また、エントリポイント入手方法の一実施形態は、前記エントリポイント検索応答ステップにおいて、エントリポイント検索メッセージの受信者が、エントリポイント検索メッセージに含まれるグループ公開鍵と応答者が保有するグループ公開鍵の比較だけでなく、検索メッセージに含まれるグループ公開鍵が、応答者が保有するグループ公開鍵更新履歴との比較によって、検索者の要求しているグループと応答者が所属しているグループの一意性を確認することを特徴とする。

【0052】

また、エントリポイント入手方法の一実施形態は、前記エントリポイント検索応答ステップにおいて、グループの一意性が確認でき、かつエントリポイント検索メッセージに含まれるグループ公開鍵が、応答者の保有する最新のグループ公開鍵でない場合に、最新のグループ公開鍵を通知することを特徴とする。

【0053】

また、エントリポイント入手方法の一実施形態は、前記エントリポイント検索応答ステップにおいて、応答者がグループ公開鍵、グループ参加証に基づいてエントリポイント検索応答メッセージを生成することを特徴とする。

【0054】

【発明の実施の形態】

まず、本発明の実施形態の構成について概要を説明する。本発明はネットワークで互いに接続された複数の機器間の通信方法に関するものである。本発明はイーサネット（R）、アナログまたはデジタルの公衆回線または専用回線を用いたネットワーク、ADSL（Asymmetric Digital Subscriber Line）、無線LAN（Local Area Network）などの物理的なネットワークを想定しているが、これらに制限されるものではない。また、インターネットではネットワークの下位プロトコルとしてTCP/IP（Transmission Control Protocol/Internet Protocol）が広く使用されており本発明もその使用を想定しているが、これに制限されるものでもない。

【0055】

前記機器のそれぞれに前記物理的なネットワークに対応した通信インタフェースが備わっており、前記通信インタフェースを制御して通信を行うためのプログラムを前記機器内のCPUが実行することにより通信処理が行われる。

【0056】

前記プログラムは前記機器のROM（Read Only Memory）に記録されている場合、あるいは前記機器のハードディスクやリムーバブルディスクなど不揮発記憶装置に格納されていてそこから必要に応じて前記機器のRAM（Random Access Memory）に読み込まれて実行される場合、あるいはこれらを組み合わせて実行する場合などがある。

【0057】

また前記機器には機器使用者の入力を受け付けるための入力手段も備わっている。入力手段としては通常キーボード、マウス、タブレットなどが用いられる。これらの構成についてはパーソナルコンピュータなどで一般的に知られているも

のであり、本発明の主眼ではないので詳細な説明は省略する。

【0058】

なお、以下で用いる「ユーザ」という用語は、前記機器、前記機器で動作するプログラムおよび機器使用者を含む概念である。

【0059】

本発明が想定しているネットワークにおいては、各ユーザは、必ずしも常時ネットワークに接続しているわけではなく、通信に必要な各ユーザのアドレス情報（IPアドレス、ポート番号など）も固定ではなくネットワークに接続するたびに変化する可能性がある。

【0060】

（実施の形態1）

本発明の第一の実施の形態について説明する。

【0061】

まず、本実施の形態で用いている公開鍵暗号化方式の概要を説明する。公開鍵暗号化方式とは、次のような数学的性質を持つ二つの暗号鍵、「公開鍵」と「秘密鍵」を用いた暗号化方式である。

【0062】

（1）公開鍵と秘密鍵は、一方から現実的な時間で他方を計算することが互いに不可能である。

【0063】

（2）公開鍵で暗号化した情報は対応する秘密鍵でのみ復号可能であり、逆もまた成立する。

【0064】

上記（1）の性質により、利用者は秘密鍵のみを秘密裡に保持しておけば、公開鍵を第三者に知られても問題ないので公開鍵を公開しておくことができる。従って、情報を秘密裡に送信したい送信者は、前もって受信者の公開鍵を入手しておき情報を受信者の公開鍵で暗号化したものを送信する。受信者は自分のみが持つ秘密鍵でそれを復号することができ、暗号化前の情報を得ることができる。第三者が暗号化された情報を傍受しても、受信者の秘密鍵でしか復号できないため

情報が漏洩することはない。以下では、暗号化対象の情報Mを鍵Kで暗号化したものを $e(M, K)$ のように表記することとする。

【0065】

また、公開鍵暗号化方式を用いて、情報そのものは暗号化しないが、情報が改ざんされていないことを証明するための電子「署名」を行うことも可能である。すなわち、署名対象の情報Mから所定のアルゴリズム f で一意に導き出される派生情報 $H = f(M)$ を送信者の秘密鍵 KS で暗号化した $Sgn = e(H, KS)$ を署名情報として元の情報Mに付加して送信する。受信者は、Mと Sgn を受信し、 Sgn を送信者の公開鍵 KP で復号化して H を得て、 $H = f(M)$ が成立することを確認することで情報Mが第三者によって改ざんされていないことを確認できる。

【0066】

なぜならば、Mが第三者により改ざんされていれば $H = f(M)$ が成立せず、また送信者の秘密鍵 KS がなければ、送信者の公開鍵 KP で正常に復号できる Sgn の作成も不可能だからである。

【0067】

公開鍵暗号化方式、およびこれを応用した署名方式は、インターネットでセキュリティを要する通信に広く用いられている。以下では、あるユーザAの公開鍵、秘密鍵をそれぞれ KA_P 、 KA_S のように表記する。

【0068】

本明細書においてグループは、次のように定義する。

【0069】

- (1) グループは一名以上のネットワーク参加者からなる
- (2) ユーザは複数のグループに属することが可能である
- (3) グループにはグループ固有の共有情報がある
- (4) 同じグループに属することを互いに認証されたメンバ間では、そのグループの共有情報の送受信を行うことができる。グループを構成するメンバは、友人、家族、同じ趣味の持ち主、住所が近い者、の集合などが考えられる。

【0070】

本実施の形態においては、グループを構成するメンバをグループ参加証を発行する権限をもつ管理者および一般ユーザに分類する。一般ユーザにグループ参加証を発行できるのは管理者のみであり、ユーザはグループ参加証を管理者に発行してもらうことでグループへの参加が可能となる。

【0071】

P2Pネットワーク上でこのようなグループを発見し、グループのメンバにアクセスするためには以下に示すような処理が必要になる。

【0072】

- (1) グループの生成
- (2) グループの告知
- (3) グループ情報の取得
- (4) エントリポイント情報の取得
- (5) グループへの新規加入依頼
- (6) グループメンバ間の認証
- (7) グループメンバ間の情報共有
- (8) グループ参加証の更新
- (9) グループメンバの削除
- (10) グループ管理者の追加
- (11) グループ公開鍵の更新

以下、各処理について説明する。

【0073】

1. グループの生成

情報共有のためにグループを作成したいユーザAは、そのグループ用の公開鍵KG_Pおよび秘密鍵KG_Sのペアを作成する。これらはAが指定した情報（パスフレーズ）を元に生成されたものであってもよいし、プログラムまたは装置が生成した乱数などの情報を元に生成されたものであってもよい。

【0074】

2. グループの告知

生成したグループ公開鍵KG_Pは、そのグループを特定するグループ識別情

報、例えば望ましくは他のグループと重複しないグループIDなどと共に何らかの方法でグループ情報として告知される。この告知方法としては、

(1) 従来の技術の説明に用いた図10にて例示したようなP2Pネットワークの全てあるいは一部のユーザを宛て先としてAがグループ情報を発信し、そのグループ情報が図15の検索情報の流れのようにユーザからユーザへと順次転送され、最終的に宛て先とされたユーザが受信することで実現してもよいし、

(2) 物理的にAと同じローカルエリアネットワーク(LAN)または仮想プライベートネットワーク(VPN)に属している他のユーザ宛てにグループ情報をブロードキャストすることで実現してもよいし、あるいは、

(3) Aが電子メール、郵便等を含む、P2Pネットワークを介した転送以外の何らかの方法で他のユーザに対して少なくともグループ公開鍵KG_Pを直接送信することで実現してもよいし、

さらには、

(4) グループ情報のリストを保持し検索の用途に供するグループ情報インデックスサーバを運営し、前記グループ情報をこのグループ情報インデックスサーバに登録することによって実現してもよいし、

(5) これらを複数組み合わせることで実現することも可能である。

【0075】

なお、前記グループ情報には、そのグループ名、グループの生成者を特定する情報、成り立ち、目的、参加条件等、当該グループの内容を説明する情報と共に告知されていても構わないし、グループ公開鍵KG_Pのみをグループ情報として告知しても構わない。

【0076】

3. グループ情報の取得

P2Pネットワークに参加しているユーザXは、次のいずれかの方法でグループを発見し、グループを特定するグループ識別情報を取得する。本実施の形態では、グループ識別情報には、少なくともグループ公開鍵KG_Pが含まれる。

【0077】

(1) Xが保持している、過去に告知され受信したグループ情報(グループを

生成したAから直接受け取ったグループ情報を含む) から、グループを特定するグループ識別情報あるいはグループを説明するグループ属性情報に基づき所望のグループを発見する。

【0078】

(2) 図10に例示したようなP2Pネットワークの情報検索の仕組みを用いて他のユーザに対してグループ識別情報あるいはグループ属性情報の一部または全部をキーとして検索し、該当するグループ情報を保持しているユーザからグループ情報を入手する。

【0079】

この際に、前述したグループ情報の詐称が問題になるが、この問題を解決するための方法の詳細は後述する。

【0080】

(3) 前記グループ情報インデックスサーバが運用されている場合には、このグループ情報インデックスサーバに対してグループ識別情報あるいはグループ属性情報の一部または全部をキーとして検索し、所望のグループのグループ情報を入手する。

【0081】

(4) グループを生成したAがXにとって既知の場合は、グループ情報をAから何らかの手段で直接入手する。

【0082】

4. エントリポイント情報の取得

グループへの参加を行う際には、グループ管理者もしくは、グループメンバを特定し、そのエントリポイント情報を入手する必要がある。グループ管理者とは、グループメンバの追加削除の権限を持つユーザであり、より具体的にはグループ秘密鍵KG_Sを保持するユーザである。あるグループへ新規加入したいユーザXは、5. で説明するようにグループ管理者Aと直接通信する必要があり、そのために必要なグループ管理者Aのエントリポイント情報を取得する必要がある。

【0083】

また、既にグループメンバとなっている場合でも、他のグループメンバと通信するために他のグループメンバのエントリポイント情報を取得する必要がある。それは例えば次のいずれかの方法で行われる。

【0084】

(1) Xは図10に例示したようなP2Pネットワークの情報検索の仕組みを用いてグループ識別情報の一部または全部をキーとして検索を行い、この検索要求を受けた該当するグループの管理者やメンバがこれに応答し、自分のアドレス情報をXに対して通知する。

【0085】

このときに前述したエントリポイント情報の詐称の問題が生じるが、これを解決するための方法についての詳細は、後述する。

【0086】

(2) 現在オンライン状態である全ユーザ、あるいは少なくとも一つのグループの管理者である全ユーザの、少なくともアドレス情報および当該ユーザが管理者であるグループのグループを特定する情報を収集して検索の用途に供するピア情報サーバが運営されている場合、Xはこのピア情報サーバに対してグループを特定する情報をキーとして検索を行い、その検索結果として管理者や、グループメンバのアドレス情報を入手する。

【0087】

(3) グループ管理者AがXにとって既知であり、かつグループ管理者Aが常にオンラインであってアドレス情報が変化しないことも既知である場合、そのアドレス情報を用いる。

【0088】

5. グループへの新規加入依頼

あるグループへ新規加入したいユーザXは、前記4. で特定したアドレス情報を用いてグループ管理者Aと通信を行い、6. で必要となるグループ参加証の発行を依頼する。

【0089】

6. グループメンバ間の認証

前記5. で入手したグループ参加証を持つグループメンバー間では、互いに同じグループに属していることを認証することが可能になる。

【0090】

7. グループメンバー間の情報共有

前記6. で互いに同じグループに属していると認証された複数のグループメンバー間、例えばXとYの間ではグループの共有情報の相互の転送が可能になる。これは、例えば次のようなステップを順に実行することにより行われる。

【0091】

(7-1) 通信に用いる暗号鍵の設定

前記6. で互いに同じグループに属していることを認証した後、暗号鍵 K_{XY} を一方、例えばX、が作成して、Xの秘密鍵およびYの公開鍵でこの暗号鍵を暗号化してYに送付する。Yはこれを自分の秘密鍵およびXの公開鍵を用いて復号可能であり、またY以外はこれを復号することができない。これにより、安全に K_{XY} をXからYに通知する。

【0092】

(7-2) 情報転送の暗号化

以降のXとYの間の情報転送は、 K_{XY} で暗号化して行う。第三者は K_{XY} を知ることができないので、XY間の通信を傍受してもその内容を復号することはできず、また、XまたはYに成りすまして偽の情報をYまたはXに転送することも不可能となり、XとYは安全に情報転送を行うことができる。これにより、グループメンバー相互間での安全なグループ情報の共有が可能となる。

【0093】

なお、3名以上のメンバーがお互いに認証された状態である場合、このメンバー間の情報転送に用いる暗号鍵には次のような選択肢がある。

【0094】

(1) 異なる二者間の通信には異なる暗号鍵を用いる。

【0095】

例えば、AとBとCが互いに認証されている場合、AとBの間の通信には暗号鍵 K_{AB} を、BC間は K_{BC} 、CA間は K_{CA} を用いる方法である。

【0096】

(2) 互いに認証された複数メンバ間で共通の暗号鍵を用いる。

【0097】

例えば、AとBが互いに認証されていて暗号鍵K_{AB}を用いて通信している状態でCが新たにAまたはBとの認証処理を行って認証された場合、AまたはBからCへCの公開鍵を用いて安全にK_{AB}を送付し、以降はA、B、Cのいずれの二者間でも暗号鍵K_{AB}を用いる方法である。

【0098】

8. グループ参加証の更新

前記5. で発行されるグループ参加証に有効期限情報が含まれている場合には、当該有効期限以降グループへの参加（グループメンバ間の認証）が不可能になるため、ユーザはグループ参加証の更新が必要となる。

【0099】

9. グループメンバの削除

上記で述べてきた方法では、グループ参加証を持つユーザは、そのグループ参加証の有効期限まではグループへの参加が可能であるが、何らかの理由により、その有効期限以前にそのユーザをグループメンバから除外したい（そのユーザをグループメンバとして認証できないようにしたい）場合は、例えば次のような処理を実行することで可能となる。

【0100】

(9-1) グループ参加証の消去

除外対象メンバが保持しているグループ参加証を消去すれば、当該メンバはその後は前記6. で述べたグループメンバ間の認証が行えなくなる。そのためには次のような処理を実行する必要がある。

【0101】

(9-1-1) グループ参加証の消去指示

グループ管理者がメンバを除外することを指定することを指示する参加証消去指示ステップを実行する。

【0102】

(9-1-2) グループ参加証の消去

上記参加証消去指示を受けた当該メンバは、自分が保持しているグループ参加証を消去する。これは機器の使用者が手動で消去する方法でも良いが、この場合は指示を無視して故意に消去しない場合も考えられるので、上記参加証消去指示を受けた機器あるいはプログラムが強制的に消去する方法でもよい。

【0103】

しかし、この方法でグループ参加証を消去するには、グループ管理者と除外対象メンバが同時にオンラインである必要があり、必ずしも除外対象メンバのグループ参加証が消去できるとは限らない。この問題を解決するには次のような方法が考えられる。

【0104】

(9-2-1) 失効者情報の作成

グループメンバの一人（グループ管理者含む）が、除外されたメンバを特定する情報、例えば当該メンバの公開鍵、を含む失効者情報を作成する。

【0105】

(9-2-2) 失効者リストの共有

前記6.のグループメンバ間の認証の際には、自分が保持する失効者情報のリストと認証相手が持つ失効者情報のリストを比較し、一方が保持しない失効者情報が存在する場合は互いに他方の失効者リストに追加することで、失効者情報のリストを全グループメンバで共有するようにする。

【0106】

(9-2-3) 失効者の除外

前記6.のグループメンバ間の認証の際に、認証相手が自分の保持する失効者リストに含まれているかどうかを確認し、含まれている場合は相手をグループメンバであると認証しない。例えばユーザの公開鍵を失効者情報として用いる場合は、認証相手の公開鍵がリストに含まれる失効者情報のいずれかと一致すれば、この相手の認証を拒否する。

【0107】

(9-2-4) 失効者の参加資格更新の拒否

前記8.においてグループ参加証の更新を行う際に、参加証の更新を依頼したユーザがリストに含まれる失効者情報のいずれかと一致するかどうかを確認し、一致するものがある場合は参加証の更新を拒否する。

【0108】

なお、失効者情報にその消去期限を含めておいて、消去期限を越えた失効者情報を削除することが可能である。例えば、グループ参加証の有効期限より少し後の時点を消去期限として付与しておけば、不要となった失効者情報を順次削除することができ、失効者情報のリストが無限に増大することを防ぐことができる。

【0109】

また、失効者情報の作成はグループ管理者のみが行い、グループ管理者がグループ秘密鍵KG_Sを用いて暗号化した状態で共有することとしてもよい。グループメンバは公開されているグループ公開鍵KG_Pを用いて失効者情報を復号することが可能であり、この失効者情報が不正に改ざんされていないことの確認が可能となる。これにより、悪意を持つユーザにより作成された不正な失効者情報が共有されることを防ぐことができる。

【0110】

10. グループ管理者の追加

前記5.で述べたグループへの新規加入は、グループ管理者がオンラインである場合にしか行えない。グループ生成直後はグループを生成したユーザー一人のみがグループ管理者であるが、グループへの新規加入の機会を増やすために、グループ管理者を増やすことが可能である。これは、グループ秘密鍵KG_Sを何らかの安全な手段、すなわち暗号化通信または郵送などの手段によってグループ管理者から別のユーザに転送することによって実現することができる。

【0111】

11. グループ公開鍵の更新

何らかの事故によりグループ秘密鍵KG_Sがグループ管理者以外のユーザに漏洩した場合、グループ秘密鍵を入手したユーザは不正にグループ参加証または失効者リストを発行することが可能となり、かつグループメンバには本来のグループ管理者が発行したグループ参加証と不正に発行されたグループ参加証を判別

することはできない。このような場合には、グループ公開鍵・秘密鍵のペアを更新する以外に不正を防ぐ方法はない。

【0112】

また、前記10.で追加されたグループ管理者のいずれかからユーザ追加削除の権限を剥奪したい場合も、グループ公開鍵・秘密鍵のペアを更新する以外の方法はない。

【0113】

一方、グループ管理者がグループ公開鍵・秘密鍵をそれぞれKG_P'、KG_S'に更新したとしても、従来のグループ公開鍵KG_Pとそれに基づいて作成されたグループ参加証を持つグループメンバー同士では前記6.のグループ認証は互いに可能なままなので、グループメンバーは常に最新のグループ公開鍵を保持しておく必要があると同時に、最新のグループ公開鍵に対応したグループ参加証を入手する必要がある。

【0114】

最新のグループ公開鍵の保持は、例えば次のいずれかのような方法により可能である。

【0115】

(1) グループ管理者がグループ公開鍵・秘密鍵を更新した時点で、図10に例示したようなP2Pネットワークを介してネットワーク参加者全員に新しいグループ公開鍵を送付する。対応するグループのメンバーは、この新しいグループ公開鍵で自分が保持しているグループ公開鍵を置き換える。

【0116】

(2) 前記2.で告知されるグループ情報に、グループ公開鍵の更新時刻に関する情報も含めておき、前記各グループメンバーはグループ公開鍵に加えてこのグループ公開鍵の更新時刻に関する情報も保持しておく。そして、前記6.のグループ認証時には双方が持つグループ公開鍵とその更新時刻の比較を行い、新しい方のグループ公開鍵で古いほうのグループ公開鍵を置き換える。

【0117】

(3) 前記2.の(4)におけるグループ情報インデックスサーバを運営して

いる場合には、グループ情報に（１）同様グループ公開鍵の更新時刻に関する情報も含めておき、グループメンバはオンラインになった時、一定時間おき、あるいは前記 6. のグループ認証を行う直前、などのタイミングで前記グループ情報インデックスサーバにアクセスして当該グループの最新のグループ公開鍵を入手する。

【0118】

最新のグループ公開鍵に対応したグループ参加証を入手するには、グループ公開鍵の更新を検出した時点で参加証の再発行依頼（前記 8.）を実行すればよい。

【0119】

（４）前記 3. の（２）もしくは、前記 4. の（１）のように、P2Pネットワークの情報検索の仕組みを用いてグループ情報やエントリポイント情報の検索が行われた際の応答として最新のグループ公開鍵を通知する。

【0120】

この場合、検索者は検索のためのメッセージに、グループ公開鍵を含めておく。グループのメンバはグループ公開鍵の履歴を保存しておき、受け取ったメッセージに含まれるグループ公開鍵が、自身のグループ公開鍵の履歴に含まれる場合に、検索の応答として、最新のグループ公開鍵を送信する。エントリポイント情報の検索に対して、最新のグループ公開鍵を通知する方法の詳細については後述する。

【0121】

次に、前記 3. で概要を述べた P2P ネットワークでの情報検索の仕組みを用いたグループ情報の取得の処理の流れについて図 1 と図 2 を参照して順を追って詳細に説明する。図 1 はグループの検索を行う検索者 X とグループ管理者 A でそれぞれ実行される処理の流れを図示したものである。図 2 はグループの検索が終了したあと、検索者 X が保持している情報をあらわしている。

【0122】

〔ステップ 101〕

事前に、グループ管理者 A はグループの公開鍵 KG__P ・ 秘密鍵 KG__S のペ

アを作成する。また、KG_Pを含むグループ情報IGを生成する。

【0123】

KG_Pおよび、IGについては公開しておいても構わない。（前記1. および前記2. を参照）。

【0124】

[ステップ102]

検索者Xは検索したいグループの条件CGを作成する。このとき指定される条件はグループのカテゴリなどが考えられるが特に規定されるものではない。また、条件記述の形式も特に限定されるものではない。

【0125】

[ステップ103]

Xは作成したCGを含むグループ検索メッセージMG_Qを生成して送信する。この時の送信方法は、ブロードキャスト、マルチキャスト、P2Pネットワークによるメッセージ伝播などで送信されるが、送信方法は特に限定されるものではない。

【0126】

[ステップ104]

Aはグループ検索メッセージMG_Qを受け取り、MG_Qに含まれるCGと自分が管理するグループのグループ情報IGとを比較し、自分が管理するグループがCGで指定される条件に適合するかを判定する。この判定は管理者が自分で判断しても良いし、プログラムなどで自動的に判定しても良い。CGとIGが適合しない場合は、AはMG_Qを破棄して処理を終了する、またはMG_Qを別のユーザに送信して処理を終了する。

【0127】

[ステップ105]

AはKG_Pを含むIGからグループ情報応答メッセージMG_Aを作成する。Aはグループ秘密鍵KG_Sを使用してMG_Aに署名を施した後、Xに向けて送信する。

【0128】

[ステップ106]

XはAからMG__Aを受け取ると、MG__Aに含まれるKG__Pを入手する。

【0129】

[ステップ107]

XはKG__Pを使用して、MG__Aの署名の有効性を確認する。署名の有効性が確認されない場合は、MG__Aは第三者によって改竄されている可能性があるために、XはMG__Aを破棄して処理を終了する。

【0130】

[ステップ108]

XはMG__AからIGを入手する。

【0131】

[ステップ109]

XはIGとCGを比較し、両者が適合するかを判定する。

【0132】

適合しないと判定した場合、XはMG__Aを破棄して、処理を終了する。

【0133】

[ステップ110]

XはAから受信したMG__Aに含まれるIGを保存する。また、必ずしも管理者がメッセージを生成するのではなく、以前に管理者が生成した応答メッセージを別のユーザがキャッシュしておき応答に使用する実施形態も考えられる。

【0134】

上記の方法を用いることによって、検索者Xは応答として入手できたグループの情報がグループ公開鍵KG__Pを有するグループの管理者によって作成されたものであることが確認できる。

【0135】

つまり、グループを一意に特定する識別子として、グループ公開鍵を使用し、グループ情報にグループ秘密鍵による署名を付加することによって、グループの管理者以外が、そのグループに関する情報を詐称することを防止することができる。

【0136】

また、仮に他のグループG2の管理者が自己のグループの識別子として、グループG1のグループ公開鍵を使用した場合にも、現状では十分な長さをもつ公開鍵から秘密鍵を計算することは事実上困難であるため、G1のグループ秘密鍵までも詐称することができない。

【0137】

この方法によって、グループ情報の詐称、グループを一意性の確認の課題を解消することができる。

【0138】

ただ、グループ公開鍵を安全性の確保のために時折更新する場合には、グループの一意性を確認するための識別子として単一のグループ公開鍵を使用することはできない。この場合には、後述するように、グループの公開鍵の履歴を使用してグループの一意性を確保する必要がある。

【0139】

次に、前記4.で概要を説明した、P2Pネットワークの情報検索の仕組みを用いたグループのエントリポイント検索について図3、図4を用いて詳細に説明する。図3は検索者Xとグループ参加者Yでそれぞれ実行される処理の流れを図示したものである。図4はエントリポイント検索が終了したあと、検索者Xが保持している情報をあらわしている。

【0140】

[ステップ301]

検索者Xはエントリポイントを手に入れたいグループのグループ公開鍵KG_Pを含むエントリポイント検索メッセージME_Qを生成して、送信する。このときの送信方法は、ブロードキャスト、マルチキャスト、ユニキャスト、P2Pネットワークによるメッセージ伝播など様々な方法が考えられるが、ここでは特定の送信方法に限定されない。

【0141】

[ステップ302]

ME_Qを受信した参加者Yは、ME_Qに含まれるKG_Pを手にし、Yが

参加しているグループの公開鍵 KG_P' と比較する。

【0142】

[ステップ303]

二つの公開鍵が一致しない場合にはYは ME_Q を破棄して処理を終了するか、もしくは、 ME_Q を別のユーザに送信して処理を終了する。

【0143】

[ステップ304]

Yは自分のグループ参加証 C_X および、自身のエントリポイント情報 E_Y を含むエントリポイント検索応答メッセージ ME_A を作成する。Yは ME_A に対して自身の秘密鍵 KY_S で署名を行い、署名された ME_A をXに送信する。

【0144】

[ステップ305]

Xは受信した ME_A から C_Y を取得する。

【0145】

[ステップ306]

Xは KG_P を使用して C_Y の有効性を確認する。簡単には(1) KG_P で正常に復号化できる、あるいは署名を確認できるか。(2)有効期限は切れていないかの二点によって C_Y の有効性は確認できる。 C_Y の有効性が確認できない場合、Xは ME_A を破棄して処理を終了する。

【0146】

[ステップ307]

C_Y からYの公開鍵 KY_P を取得する。 KY_P を使用して、 ME_A の署名を確認する。

【0147】

[ステップ308]

ME_A の署名の正当性が確認できない場合、 ME_A は第三者によって改竄された可能性があるため、Xは ME_A を破棄して処理を終了する。

【0148】

[ステップ309]

XはYをKG_Pによって特定されるグループのメンバであると認定し、EYをグループのエントリポイントとして記憶する。

【0149】

上記の方法のように、グループを一意に識別する情報としてグループ公開鍵を使用し、応答にグループ公開鍵で指定されるグループのメンバであることを証明する情報を含めることによって、グループメンバ以外のユーザがエントリポイント情報を詐称することを防ぐことができる。

【0150】

次に、前記11.の(4)で概要を説明した、グループ公開鍵の更新方法について図5、図6を参照して順をおって詳細に説明する。図5はエントリポイント検索者Xとそのグループ公開鍵に対応するグループの参加者Yでそれぞれ実行される処理の流れを図示したものである。図6はグループ公開鍵の通知を受けたあと、検索者Xが保持している情報をあらわしている。

【0151】

[ステップ501]

検索者Xはエントリポイントを入手したいグループのグループ公開鍵KG_Pを含むエントリポイント検索メッセージME_Qを生成して、送信する。このときの送信方法は、ブロードキャスト、マルチキャスト、ユニキャスト、P2Pネットワークによるメッセージ伝播などが用いられるが、ここでは特定の送信方法に限定しない。

【0152】

[ステップ502]

ME_Qを受信した参加者Yは、ME_Qに含まれるKG_Pを入手する。

【0153】

[ステップ503]

Yは自分が参加しているグループの公開鍵KG_P'とKG_Pを比較する。このとき、二つの公開鍵が一致する場合には、前記図3のステップ304以降の処理を実行する。

【0154】

[ステップ504]

YはKG_Pが、自分が属しているグループ公開鍵の履歴HGに含まれているかを判定する。

【0155】

[ステップ505]

KG_PがHGに含まれていない場合にはYはME_Qを破棄して処理を終了する、もしくは、ME_Qを別のユーザに送信して処理を終了する。

【0156】

[ステップ506]

YはHGと共に、履歴に対応するグループ公開鍵変更メッセージを所有している。グループ公開鍵がKG_P(I)からKG_P(I+1)に変更される場合には、グループ管理者から、グループ公開鍵変更メッセージMC_K(I)が、グループメンバに通知される。MC_K(I)は、KG_P(I+1)を含み、それに対してKG_P(I)、KG_P(I+1)で署名されており、以前のグループ秘密鍵、および最新のグループ秘密鍵を所有する管理者が発行したことが確認できる。

【0157】

KG_PがグループのI番目の鍵、KG_P'がグループのI+J番目の鍵であった場合、YはMC_K(I+1)からMC_K(I+J)までJ個のグループ公開鍵変更メッセージを含むグループ公開鍵通知メッセージMU_Kを作成し、Xに送信する。

【0158】

[ステップ507]

Xは受信したMU_Kを受信し、K=1として以降の処理を実行する。

【0159】

[ステップ508]

Xは受信したMU_Kから、MC_K(I+K)を取得する。

【0160】

【ステップ509】

Xは $KG_P(I+K-1)$ を使用して、 $MC_K(I+K)$ の署名を確認する。

【0161】

【ステップ510】

署名の正当性が確認されない場合は、 MU_K を破棄して処理を終了する。

【0162】

【ステップ511】

証明の正当性が確認できた場合は、 $MC_K(I+K)$ から、 $KG_P(I+K)$ を取得する。

【0163】

【ステップ512】

KとJが等しいかを判定する。KがJと等しくない場合はステップ513の処理を、KとJが等しい場合はステップ514の処理を実行する。

【0164】

【ステップ513】

$K=K+1$ として、ステップ508以降の処理を繰り返す。

【0165】

【ステップ514】

$KG_P' = KG_P(I+J)$ を最新のグループ公開鍵として KG_P と置き換える。

【0166】

上記の方法のように、グループ公開鍵の履歴によってグループの一意性を判定することによってグループ公開鍵のように更新される情報をグループの識別子として使用することが可能になる。

【0167】

また、上記の手法をとることで、古いグループの公開鍵しか所有していないユーザであっても最新のグループ公開鍵の通知を受けることができ、通知された最新のグループ公開鍵の正当性を以前のグループ公開鍵によって確認することがで

きる。

【0168】

上記に述べたように、グループに対して固有のグループ公開鍵を設定することで、グループの一意性の確認の問題、グループに対する情報の詐称の問題を解決することができる。

【0169】

(実施の形態2)

前述した第一の実施の形態では、グループを構成するメンバとしては管理者と一般ユーザだけとしているが、第一の実施の形態の10. で述べたように、グループメンバの新規加入機会を増やすためには管理者を増やす、すなわちグループ秘密鍵を複製することが必要であるが、グループ秘密鍵が複数のユーザに保持されることで、漏洩する可能性が高くなるという課題がある。

【0170】

本実施の形態はこれを改善するものであり、グループを構成するメンバを唯一の管理者、グループ参加証発行許可証を保持し、グループ参加証を発行する権限を持つ発行者、および一般ユーザに分類する。発行者に権限を与えることができるのは管理者のみであり、一般ユーザにグループ参加証を発行できるのは管理者および発行者である。こうすることにより、管理者が複数の発行者を設けておけば、グループの秘密鍵を複製することなくユーザの新規加入機会を増やすことが可能となる。

【0171】

このようなグループを管理するには、以下に示すような処理が必要となる。

【0172】

- (1) グループの生成
- (2) グループの告知
- (3) グループ発行者の追加
- (4) グループ情報の取得
- (5) エントリポイント情報の取得
- (6) グループへの新規加入依頼

- (7) グループメンバー間の認証
- (8) グループメンバー間の情報共有
- (9) グループ参加証の更新
- (10) グループ参加証発行許可証の更新
- (11) グループメンバーの削除
- (12) グループ公開鍵の更新

以下、各処理について説明する。ただし、第一の実施の形態と同一のものについてはその旨記して説明を省略している。

【0173】

1. グループの生成

第一の実施の形態の1. グループの生成と同じであるので省略する。

【0174】

2. グループの告知

第一の実施の形態の2. グループの告知と同じであるので省略する。

【0175】

3. グループ発行者の追加

前記1. でグループを生成したユーザ（グループ管理者）は、グループ参加証発行許可証を発行することでグループメンバーを追加する権限を持つユーザを必要人数追加することができる。すなわち、グループ参加証発行許可証を発行されたユーザは他のユーザに対してグループ参加証を発行することが可能となる。グループ管理者がグループ参加証発行許可証を発行したユーザをグループ発行者と呼ぶ。

【0176】

4. グループの発見

P2Pネットワークに参加しているユーザXは、次のいずれかの方法でグループを発見し、グループを特定するグループ識別情報を取得する。本実施の形態では、グループ識別情報には、少なくともグループ公開鍵KG_Pが含まれる。

【0177】

- (1) Xが保持している、過去に告知され受信したグループ情報（グループを

生成したAから直接受け取ったグループ情報を含む) から、グループを特定するグループ識別情報あるいはグループを説明するグループ属性情報に基づき所望のグループを発見する。

【0178】

(2) 図10に例示したようなP2Pネットワークの情報検索の仕組みを用いて他のユーザに対してグループ識別情報あるいはグループ属性情報の一部または全部をキーとして検索し、該当するグループ情報を保持しているユーザからグループ情報を入手する。

【0179】

この際に、前述したグループ情報の詐称が問題になるが、この問題を解決するための方法の詳細は後述する。

【0180】

(3) 前記グループ情報インデックスサーバが運用されている場合には、このグループ情報インデックスサーバに対してグループ識別情報あるいはグループ属性情報の一部または全部をキーとして検索し、所望のグループのグループ情報を入手する。

【0181】

(4) グループを生成したAがXにとって既知の場合は、グループ情報をAから何らかの手段で直接入手する。

【0182】

5. エントリポイントの特定

グループへの参加を行う際には、グループ管理者、グループ発行者もしくは、グループメンバを特定し、そのエントリポイント情報を入手する必要がある。あるグループへ新規加入したいユーザXは、5. で説明するようにグループ発行者Bと直接通信する必要があり、そのために必要なグループ発行者Bのエントリポイント情報を取得する必要がある。

【0183】

また、既にグループメンバとなっている場合でも、他のグループメンバと通信するために他のグループメンバのエントリポイント情報を取得する必要がある。

それは例えば次のいずれかの方法で行われる。

【0184】

(1) Xは図10に例示したようなP2Pネットワークの情報検索の仕組みを用いてグループ識別情報の一部または全部をキーとして検索を行い、この検索要求を受けた該当するグループの発行者やメンバがこれに応答し、自分のアドレス情報をXに対して通知する。このときに前述したエントリポイント情報の詐称の問題が生じるが、これを解決するための方法についての詳細は、後述する。

【0185】

(2) 現在オンライン状態である全ユーザ、あるいは少なくとも一つのグループの管理者である全ユーザの、少なくともアドレス情報および当該ユーザが管理者であるグループのグループを特定する情報を収集して検索の用途に供するピア情報サーバが運営されている場合、Xはこのピア情報サーバに対してグループを特定する情報をキーとして検索を行い、その検索結果として管理者や、グループメンバのアドレス情報を入手する。

【0186】

(3) グループ発行者BがXにとって既知であり、かつグループ発行者Bが常にオンラインであってアドレス情報が変化しないことも既知である場合、そのアドレス情報を用いる。

【0187】

6. グループへの新規加入依頼

グループへ新規加入したいユーザXは、前記5. で特定したアドレス情報を用いてグループ発行者と通信を行い、7. で必要となるグループ参加証の発行を依頼する。

【0188】

7. グループメンバ間の認証

前記6. で入手したグループ参加証を持つグループメンバ間では、互いに同じグループに属していることを認証することが可能になる。

【0189】

8. グループメンバ間の情報共有

第一の実施の形態の前記7.と同じであるので省略する。

【0190】

9. グループ参加証の更新

前記6. で発行されるグループ参加証に有効期限情報が含まれている場合には、当該有効期限以降グループへの参加（グループメンバー間の認証）が不可能になるため、ユーザはグループ参加証の更新が必要となる。

【0191】

10. グループ参加証発行許可証の更新

前記3. で発行されたグループ参加証発行許可証に有効期限情報が含まれている場合には、当該有効期限以降グループ参加証の発行が不可能になるため、発行者はグループ参加証発行許可証の更新が必要となる。

【0192】

11. グループメンバーの削除

第一の実施の形態同様、何らかの理由により、グループ参加証の有効期限以前に特定のメンバーをグループメンバーから除外したい場合がありえる。

【0193】

当該メンバーのグループ参加証を消去する方法は、第一の実施の形態の前記9. における方法において「グループ管理者」を「グループ管理者またはグループ発行者」に置き換えた場合と同一であるので詳細な説明は省略する。

【0194】

第一の実施の形態同様、失効者情報を作成・共有する方法をとることも可能である。すなわち、例えば次のような処理を実行する。

【0195】

(11-1) 失効者情報の作成

グループメンバーの一人（グループ管理者、グループ発行者含む）が、除外されたメンバーを特定する情報、例えば当該メンバーの公開鍵、を含む失効者情報を作成する。

【0196】

(11-2) 失効者リストの共有

前記 7. のグループメンバー間の認証の際には、自分が保持する失効者情報のリストと認証相手が持つ失効者情報のリストを比較し、一方のリストに含まれない失効者情報が存在する場合は互いに他方のリストに追加することで、失効者情報のリストを全グループメンバーで共有するようにする。

【0197】

(11-3) 失効者の除外

前記 7. のグループメンバー間の認証の際に、認証相手が自分の保持する失効者情報のリストに含まれているかどうかを確認し、含まれている場合は相手をグループメンバーであると認証しない。例えばユーザの公開鍵を失効者情報として用いる場合は、認証相手の公開鍵がリストに含まれる失効者情報のいずれかと一致すれば、この相手の認証を拒否する。

【0198】

(11-4) 失効者の参加資格更新の拒否

前記 9. においてグループ参加証の更新を行う際に、参加証の更新を依頼したユーザがリストに含まれる失効者情報のいずれかと一致するかどうかを確認し、一致するものがある場合は参加証の更新を拒否する。

【0199】

なお、失効ユーザ情報にその消去期限を含めておいて、消去期限を越えた失効者情報を削除することが可能であるのは第一の実施の形態同様である。

【0200】

また、第一の実施の形態同様、失効者情報の作成はグループ発行者のみが行い、グループ発行者が自分の秘密鍵を用いて暗号化した状態で共有することとしてもよい。グループメンバーは失効者情報とそれを発行したグループ発行者の参加証発行許可証を同時に入手することにより、この参加証発行許可証に含まれるグループ発行者の公開鍵を用いて失効者情報を復号することが可能であり、この失効者情報が不正に改ざんされていないことの確認が可能となる。これにより、悪意を持つユーザにより作成された不正な失効者情報が共有されることを防ぐことができる。

【0201】

12. グループ公開鍵の更新

何らかの事故によりグループ秘密鍵 KG_S がグループ管理者以外のユーザに漏洩した場合、グループ秘密鍵を入手したユーザは不正にグループ参加証発行許可証を発行することが可能となり、ひいてはグループ参加証を不正に発行することが可能となる。このときグループメンバには不正なグループ参加証発行許可証やグループ参加証と正規のものを判別することはできない。このような場合には、グループ公開鍵・秘密鍵のペアを更新する以外に不正を防ぐ方法はない。

【0202】

一方、グループ管理者がグループ公開鍵・秘密鍵をそれぞれ KG_P' 、 KG_S' に更新したとしても、従来のグループ公開鍵 KG_P とそれに基づいて作成されたグループ参加証発行許可証を持つグループメンバ同士では前記6. のグループ認証は互いに可能なままなので、グループメンバは常に最新のグループ公開鍵を保持しておく必要があると同時に、最新のグループ公開鍵に対応したグループ参加証を入手する必要がある。発行者はこれに加えて最新のグループ鍵に対応したグループ参加証発行許可証を入手する必要がある。

【0203】

最新のグループ公開鍵の保持は、第一の実施の形態同様、例えば次のいずれかのような方法により可能である。

【0204】

(1) グループ管理者がグループ公開鍵・秘密鍵を更新した時点で、図15に例示したようなP2Pネットワークを介してネットワーク参加者全員に新しいグループ公開鍵を送付する。対応するグループのメンバは、この新しいグループ公開鍵で自分が保持しているグループ公開鍵を置き換える。

【0205】

(2) 前記2. で告知されるグループ情報に、グループ公開鍵の更新時刻に関する情報も含めておき、前記各グループメンバはグループ公開鍵に加えてこのグループ公開鍵の更新時刻に関する情報も保持しておく。そして、前記6. のグループ認証時には双方が持つグループ公開鍵とその更新時刻の比較を行い、新しい方のグループ公開鍵で古いほうのグループ公開鍵を置き換える。

【0206】

(3) 前記2. の(4)におけるグループ情報インデックスサーバを運営している場合には、グループ情報に(1)同様グループ公開鍵の更新時刻に関する情報も含めておき、グループメンバはオンラインになった時、一定時間おき、あるいは前記6. のグループ認証を行う直前、などのタイミングで前記グループ情報インデックスサーバにアクセスして当該グループの最新のグループ公開鍵を入手する。

【0207】

最新のグループ公開鍵に対応したグループ参加証発行許可証を入手するには、グループ公開鍵の更新を検出した時点で参加証の再発行依頼(前記10.)を実行すればよい。

【0208】

最新のグループ公開鍵に対応したグループ参加証を入手するには、グループ公開鍵の更新を検出した時点で参加証の再発行依頼(前記10.)を実行すればよい。

【0209】

次に、前記4. で概要を述べたP2Pネットワークの情報検索の仕組みを利用したグループ情報の取得の処理の流れについて図7を参照して順を追って詳細に説明する。図7はグループの検索を行う検索者Xとグループ発行者Bでそれぞれ実行される処理の流れを図示したものである。グループの検索が終了したあと、検索者Xが保持している情報は図2と同じである。

【0210】

[ステップ701]

Bはグループ管理者から、グループ参加証発行許可証I__B、およびグループ公開鍵KG__Pを含むグループ情報IGを入手する。

【0211】

[ステップ702]

検索者Xは検索したいグループの条件CGを作成する。このとき指定される条件はグループのカテゴリなどが考えられるが、特に規定されるものではない。ま

た、条件記述の形式も特に限定されるものではない。

【0212】

[ステップ703]

Xは作成したCGを含むグループ検索メッセージMG_Qを生成して送信する。この時の送信方法は、ブロードキャスト、マルチキャスト、P2Pネットワークによるメッセージ伝播などを用いて送信されるが、特定の送信方法に限定されるものではない。

【0213】

[ステップ704]

Bはグループ検索メッセージMG_Qを受け取り、MG_Qに含まれるCGと自分が管理するグループのグループ情報IGとを比較し、自分が管理するグループがCGで指定される条件に適合するかを判定する。この判定は管理者が自分で判断しても良いし、プログラムなどで自動的に判定しても良い。CGとIGが適合しない場合は、BはMG_Qを破棄して処理を終了するか、あるいはMG_Qを別のユーザに送信して処理を終了する。

【0214】

[ステップ705]

Bはグループ公開鍵KG_Pを含むIG、Bのグループ参加証発行許可証I_Bを含む、グループ情報応答メッセージMG_Aを作成する。その後、Bの秘密鍵KB_Sを使用してMG_Aに署名を施した後、Xに向けて送信する。

【0215】

[ステップ706]

XはBからのグループ情報応答メッセージMG_Aを受け取ると、MG_Aに含まれるKG_PおよびI_Bを入手する。

【0216】

[ステップ707]

XはKG_Pを使用して、I_Bの有効性を確認する。簡単には、KG_Pを使用して

(1) I_Bが正常に復号化される、もしくはI_Bの署名が確認できる

(2) I__Bの有効期限が切れていない

の2点を確認することによってI__Bの有効性を確認できる。I__Bの有効性が確認されない場合は、MG__Aは正規の発行者以外によって生成されている可能性があるために、XはMG__Aを破棄して処理を終了する。

【0217】

[ステップ708]

XはI__BからBの公開鍵KB__Pを入手する。

【0218】

[ステップ709]

XはKB__Pを使用して、MG__Aの署名の有効性を確認する。署名の有効性が確認されない場合は、MG__Aは第三者によって改竄されている可能性があるために、XはMG__Aを破棄して処理を終了する。

【0219】

[ステップ710]

XはAから受信したMG__Aに含まれるIGを保存する。

【0220】

上記の方法を用いることによって、グループの発行者、グループの管理者以外がグループ情報の改竄を行うことを防ぐことができる。

【0221】

また、グループを一意に識別する情報にグループ公開鍵を使用することができることは第一の実施の形態におけるグループ情報取得の例で述べた通りである。

【0222】

なお、必ずしも管理者がメッセージを生成するのではなく、以前に管理者が生成した応答メッセージを別のユーザがキャッシュしておき応答に使用する実施形態も考えられる。

【0223】

次に、前記4.で概要を説明した、P2Pネットワークの情報検索の仕組みを使用したエントリポイントの特定の処理の流れについて図8、図9を参照して順を追って詳細に説明する。図8は検索者Xとグループの参加者Yでそれぞれ実行

される処理の流れを図示したものである。本実施の形態では参加者Yのグループ参加証は、グループ発行者Bによって発行されている。図9はエントリポイントの検索が終了した後、検索者Xが保持している情報をあらわしている。

【0224】

[ステップ801]

検索者Xはエントリポイントを入手したいグループのグループ公開鍵KG__Pを含むエントリポイント検索メッセージME__Qを生成して、送信する。このときの送信方法は、ブロードキャスト、マルチキャスト、ユニキャスト、P2Pネットワークによるメッセージ伝播などで送信されるが、ここでは特定の送信方法を想定していない。

【0225】

[ステップ802]

ME__Qを受信した参加者Yは、ME__Qに含まれるKG__Pを入手する。

【0226】

[ステップ803]

Yは自分が参加しているグループの公開鍵KG__P'とKG__Pを比較する。二つの公開鍵が一致しない場合にはYはME__Qを破棄して処理を終了する、あるいはME__Qを別のユーザに送信して処理を終了する。

【0227】

[ステップ804]

Yは自分のグループ参加証C__Y、C__Yを発行したグループ発行者Bのグループ参加証発行許可証I__BおよびYのエントリポイント情報EYを含むエントリポイント検索応答メッセージME__Aを作成する。YはME__Aに対して自身の秘密鍵KY__Sで署名を行い、署名されたME__AをXに送信する。

【0228】

[ステップ805]

Xは受信したME__AからI__Bを取得し、KG__Pを使用してI__Bの有効性を検証する。

【0229】

[ステップ 806]

I__Bの有効性が確認できない場合、Yはグループに属していないとみなされ、XはME__Aを破棄して処理を終了する。

【0230】

[ステップ 807]

Xは有効性を確認したI__BからBの公開鍵KB__Pを取得する。同時にME__AからC__Yを取得し、KB__Pを使用してC__Yの有効性を検証する。

【0231】

[ステップ 808]

C__Yの有効性が確認できない場合、Yはグループに属していないとみなされ、XはME__Aを破棄して処理を終了する。

【0232】

[ステップ 809]

XはC__YからYの公開鍵KY__Pを取得して、ME__Qの署名を確認する。

【0233】

[ステップ 810]

署名の正当性が確認されない場合は、ME__Qは第三者によって改竄されている可能性があるので、XはME__Qを破棄して処理を終了する。

【0234】

[ステップ 811]

XはYをKG__Pによって特定されるグループのメンバであると認定し、ME__AからEYを取得し、グループのエントリポイントとして記憶する。

【0235】

上記の方法を用いることによって、グループのメンバ以外がエントリポイント情報を作成したのがグループのメンバであることを確認することができる。

【0236】

【発明の効果】

本発明によれば、以下の利点を持つネットワーク上のグループの検索が可能となる。すなわち、

- (1) 常時稼動しているサーバの運用が不要であり、
- (2) 検索結果を応答者の秘密鍵、グループ参加証などから生成することにより、グループメンバ以外が検索に対する応答を生成することが出来なくなる。

【 0 2 3 7 】

これにより、グループのメンバ以外がグループの情報を詐称することを防ぐことができ、サーバがない状況においても、信頼性のある検索を実行することができる。

【図面の簡単な説明】

【図 1】

本発明の第一の実施の形態におけるグループの発見の流れを示す図

【図 2】

本発明の第一の実施の形態においてグループ情報検索者 X が保持する情報を示す図

【図 3】

本発明の第一の実施の形態におけるグループのエントリポイント検索の処理の流れを示す図

【図 4】

本発明の第一の実施の形態におけるエントリポイント検索者 X が保持する情報を示す図

【図 5】

本発明の第一の実施の形態における検索に対して、最新のグループ公開鍵を通知する処理の流れを示す図

【図 6】

本発明の第一の実施の形態においてエントリポイント検索者 X が保持する情報を示す図

【図 7】

本発明の第二の実施の形態におけるグループの発見処理の流れを示す図

【図 8】

本発明の第二の実施の形態におけるグループのエントリポイント検索の処理の

流れを示す図

【図 9】

本発明の第二の実施の形態においてエントリポイント検索者が保持する情報を示す図

【図 1 0】

P 2 P ネットワークに参加しているユーザ間での情報転送の流れを表した概念図

【図 1 1】

P 2 P ネットワークにおけるグループ情報検索の流れを表した概念図

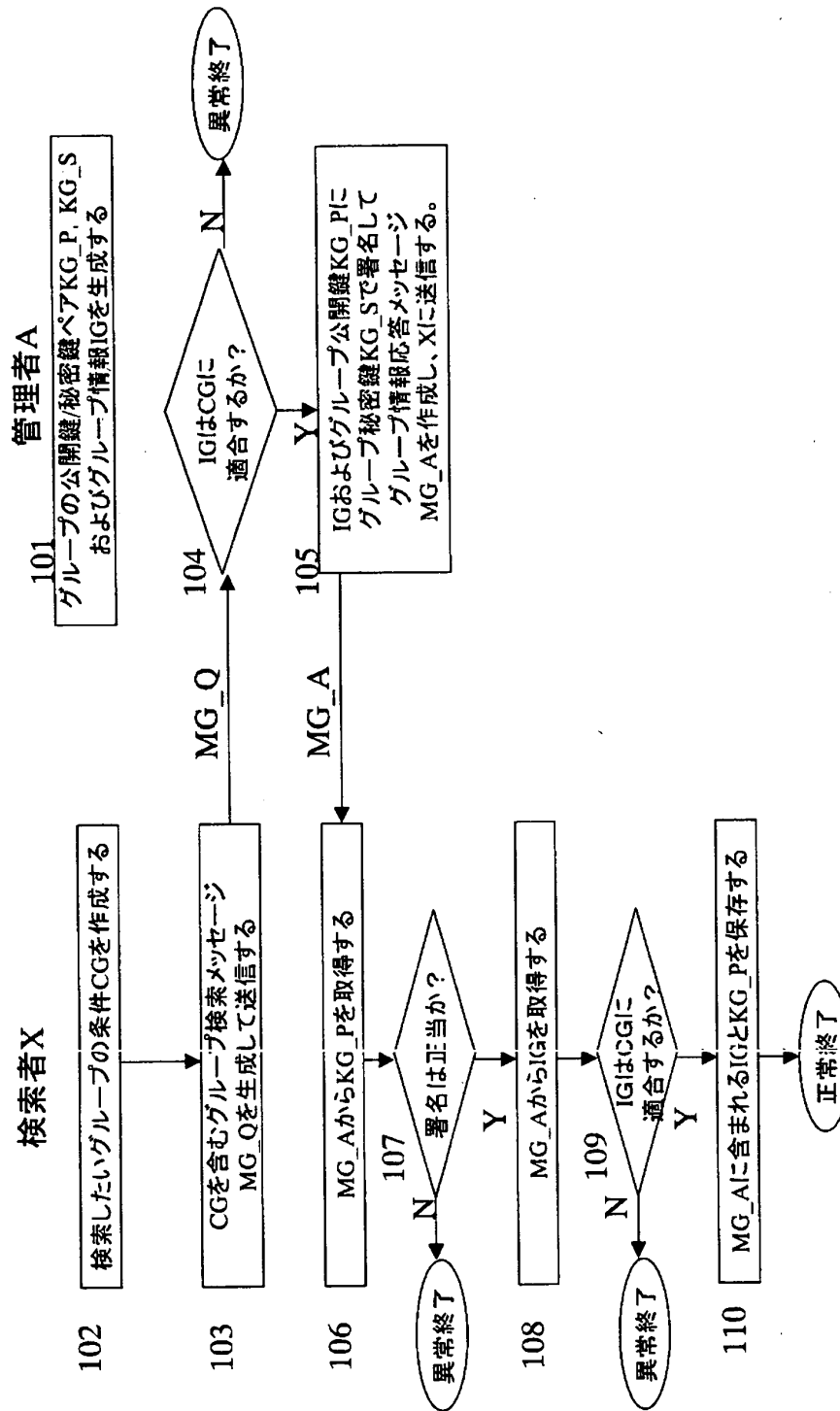
【図 1 2】

P 2 P ネットワークにおけるグループ情報検索の問題点を図示した概念図

【書類名】

図面

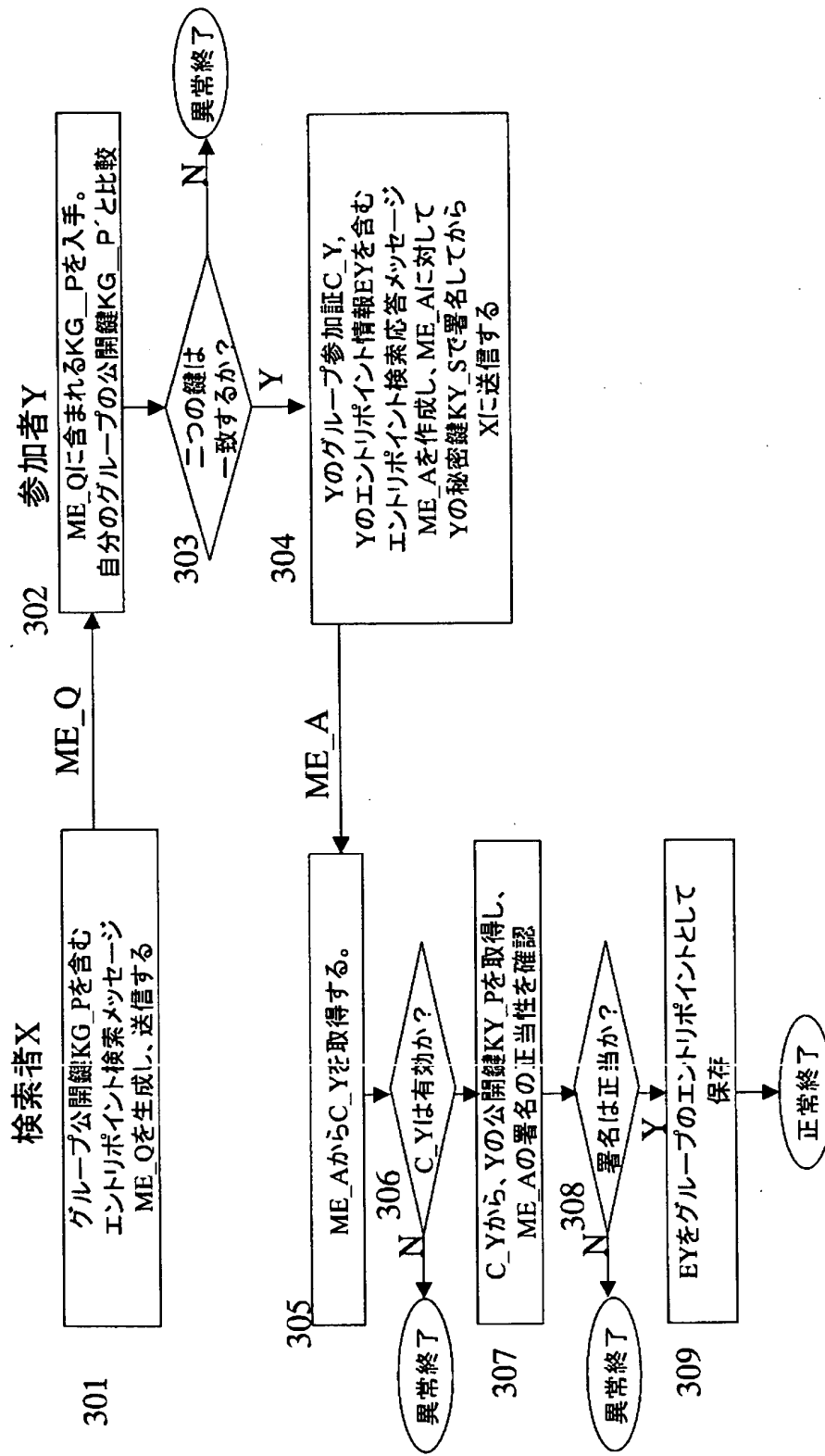
【図 1】



【図 2】

KG_P: グループの公開鍵
IG: グループに関する情報
(カテゴリや、参加に必要な情報など)

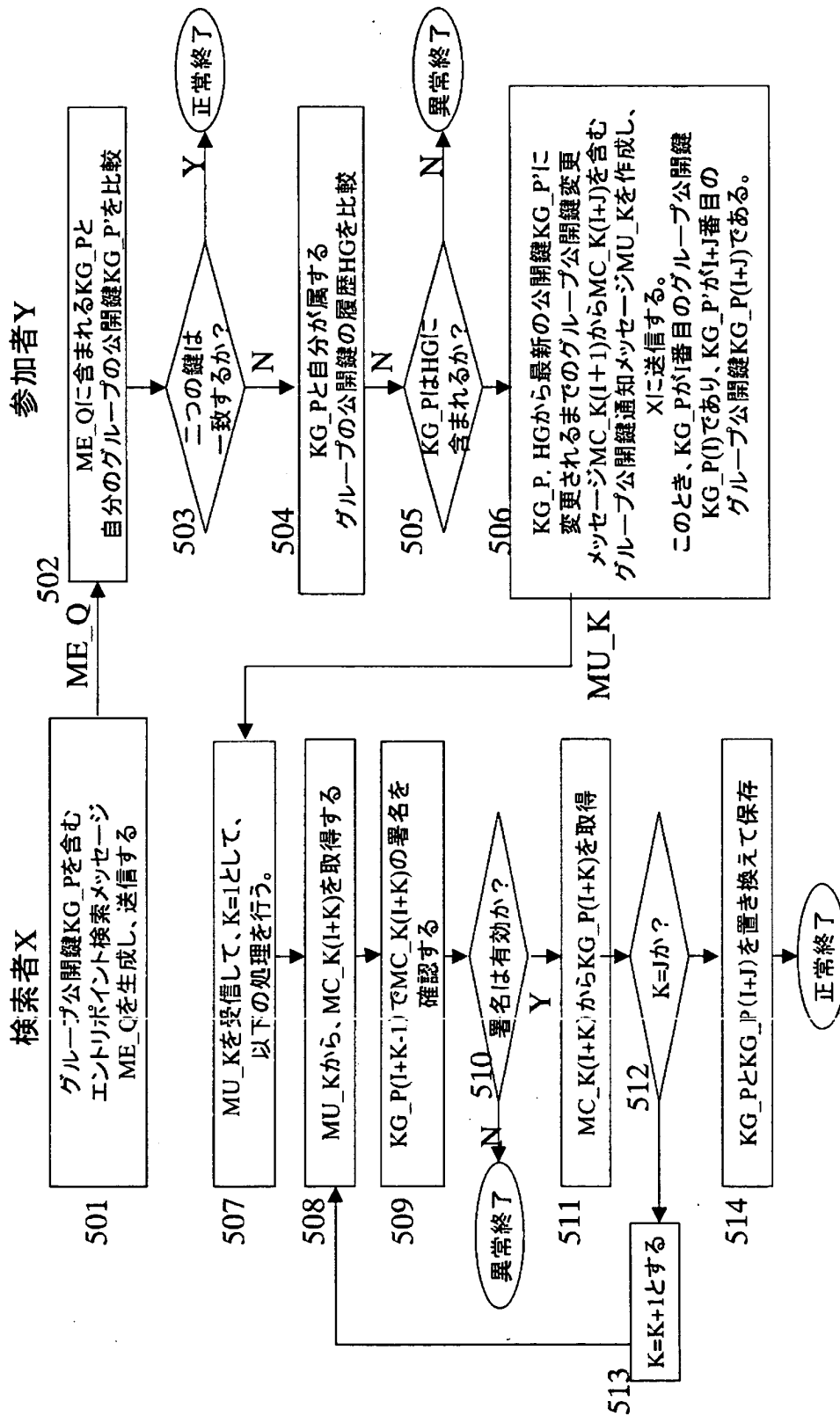
【図 3】



【図4】

EY:Yのエントリポイント情報
(IPアドレスやポート番号など)
C_Y:Yのグループ参加証

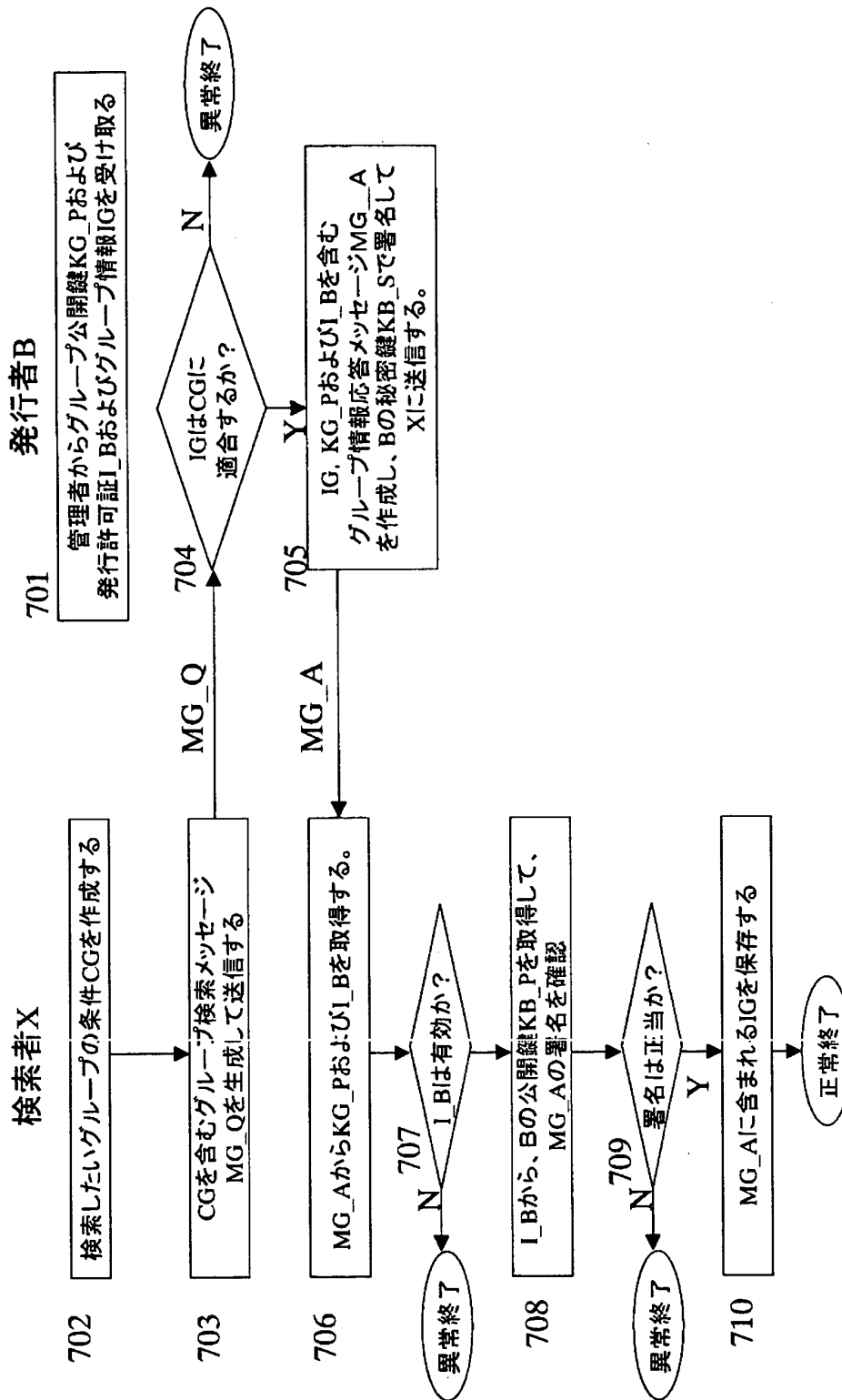
【図5】



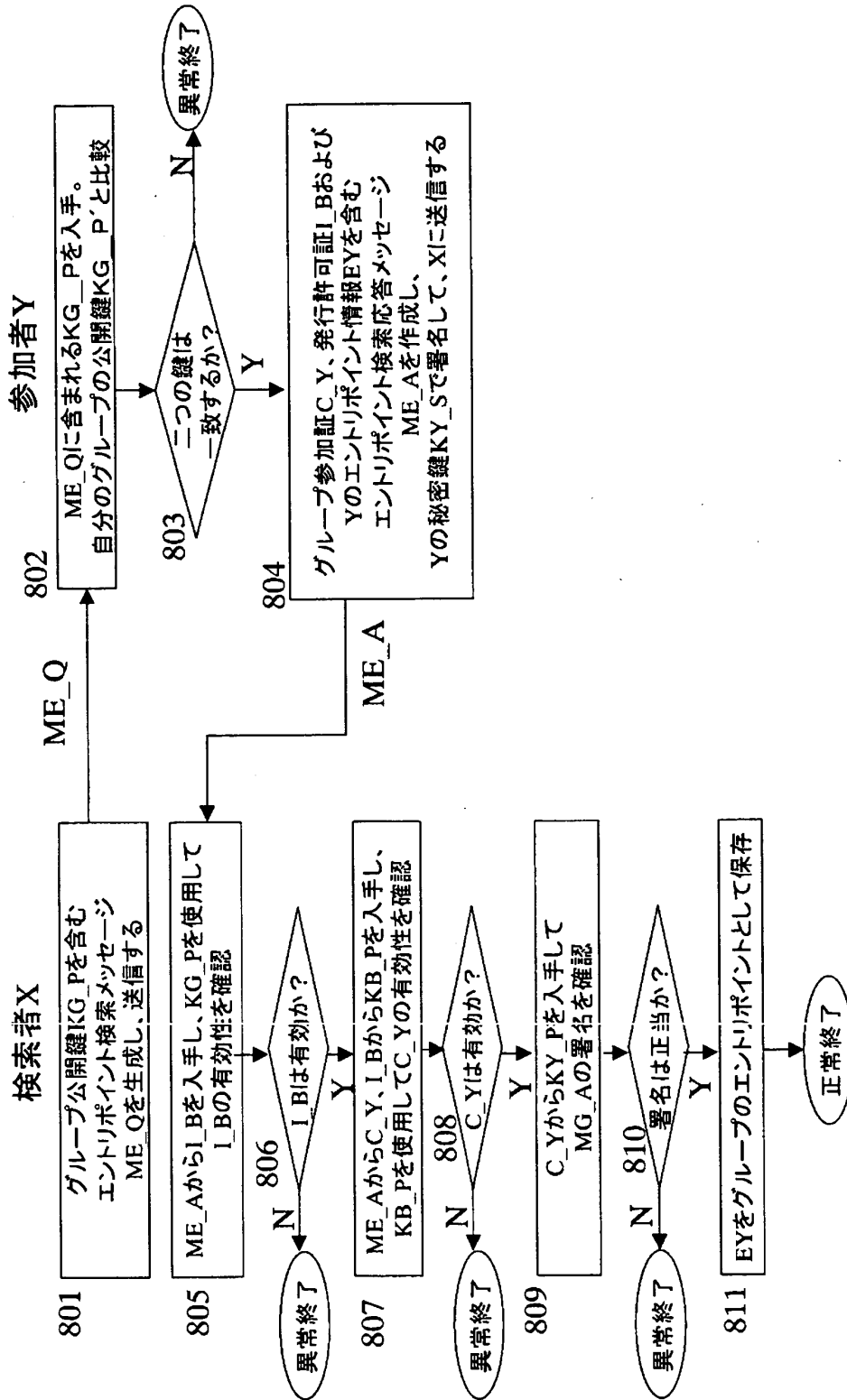
【図 6】

KG_P':最新のグループ公開鍵

【図 7】



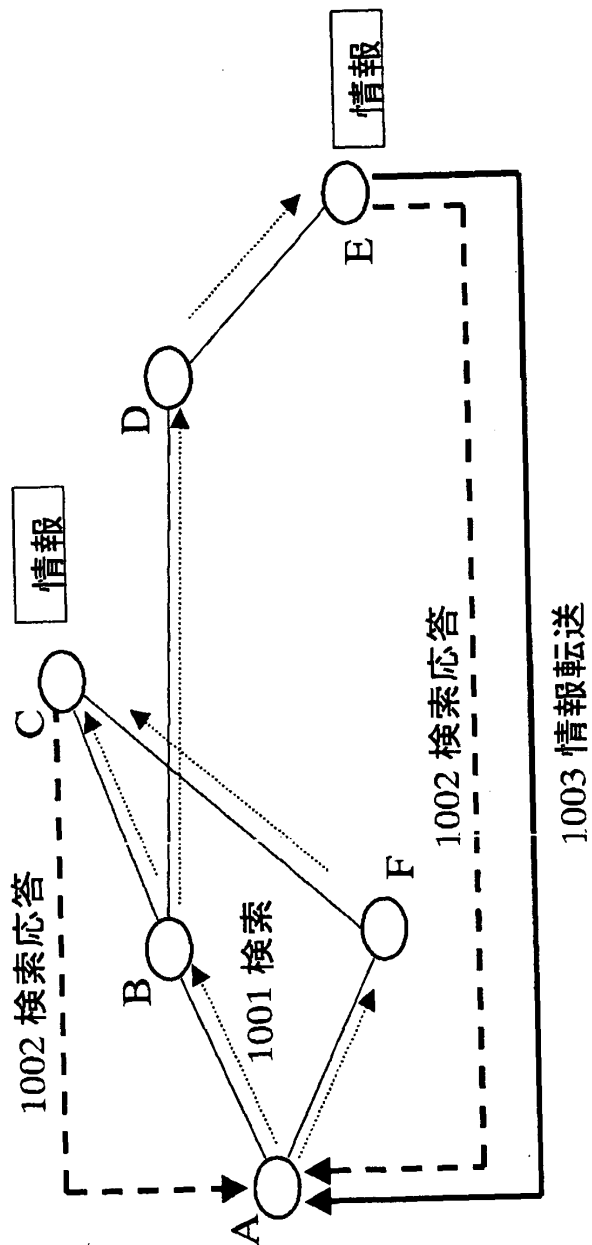
【図 8】



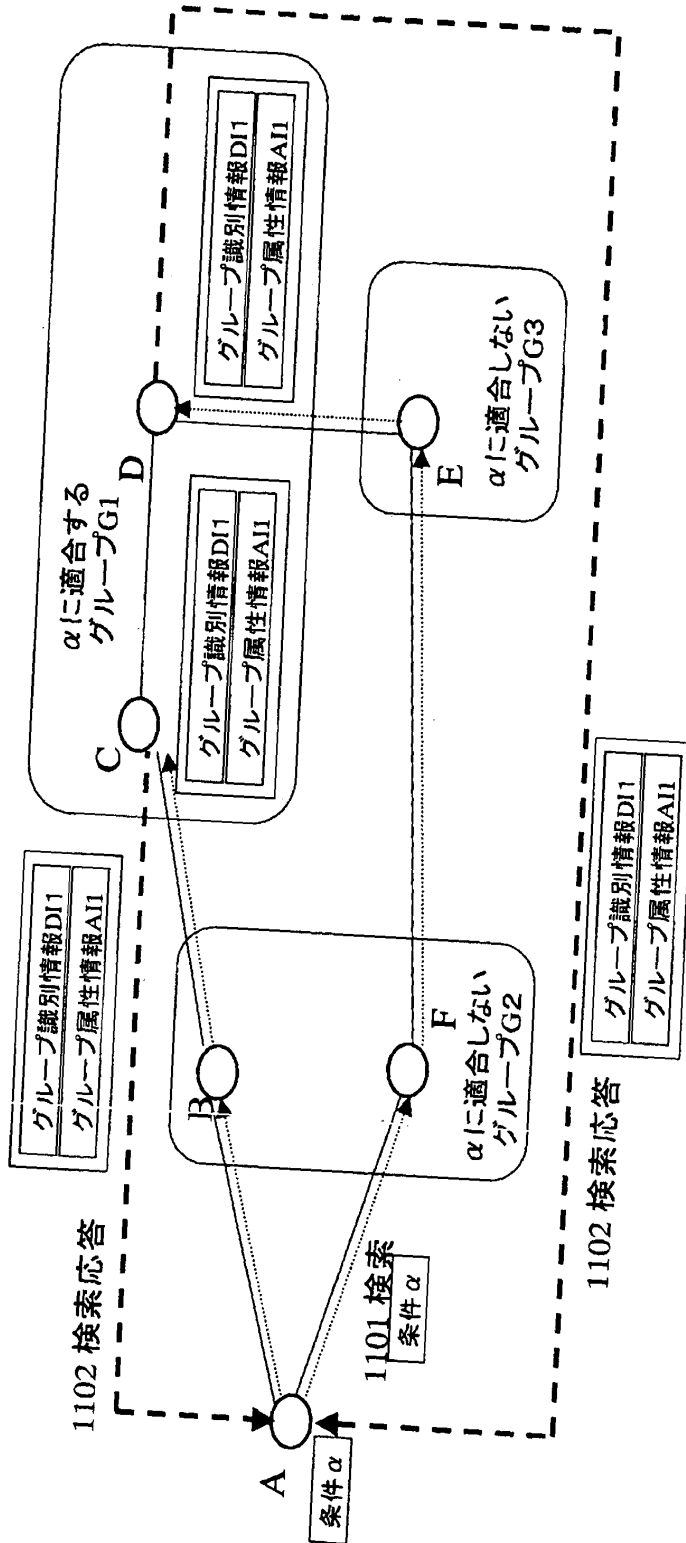
【図9】

EY: Yのエントリポイント情報
(IPアドレスやポート番号など)
C_Y: Yのグループ参加証
I_B: Bのグループ参加証発行許可証

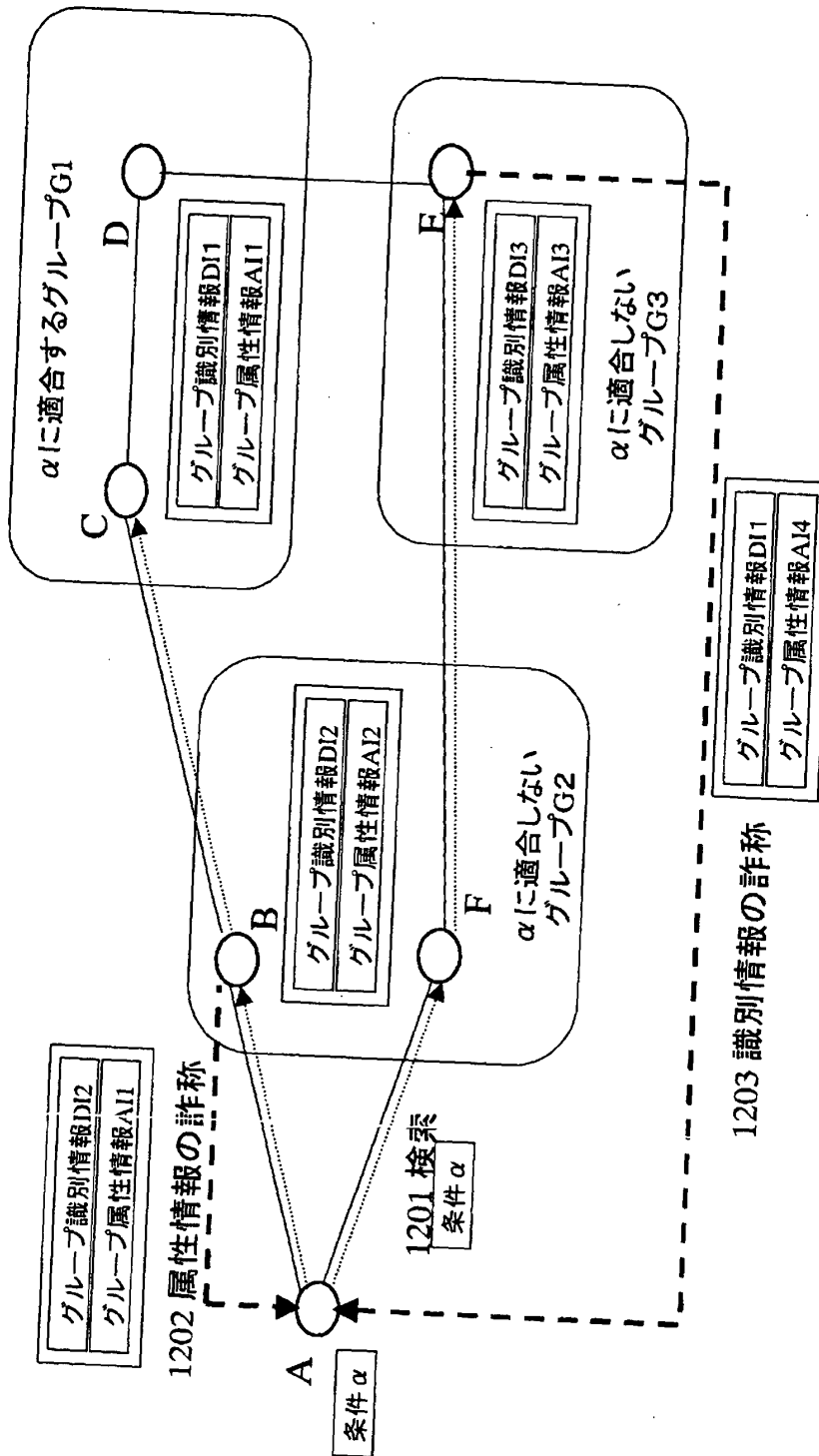
【図10】



【図11】



【図12】



【書類名】 要約書

【要約】

【課題】 Peer-to-Peerネットワークでは情報がサーバなどにより、集中管理されていないために、あるグループの情報を第三者が詐称することが容易にできる。

【解決手段】 グループの情報に対する検索に対して、管理者あるいは発行者がグループ秘密鍵もしくは発行者の秘密鍵に基づく応答メッセージを作成する。またグループのエントリポイントに対する検索に対して、グループのメンバが持つ参加証に基づく応答メッセージを作成し、検索応答がグループのメンバからのものであることを保証する仕組みを導入する。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日
[変更理由] 新規登録
住 所 大阪府門真市大字門真1006番地
氏 名 松下電器産業株式会社